Kommentar zum Europäischen Datenschutztag am 28. Januar 2020

von Matthias Canisius, Director Central & Eastern Europe, SentinelOne

Die aktuellen Schlagzeilen rund um den Leak von 515.000 Zugangsdaten für Router, Server und Smart-Home-Geräte, die ein Hacker ausgespäht und in einem Forum für Cyberkriminelle veröffentlicht hat, hat uns gleich zu Beginn des Jahres wieder einmal gezeigt, wie schnell sensible Daten in die falschen Hände geraten können. Da passt es, dass in wenigen Tagen, am 28. Januar, der Europäische Datenschutztag begangen wird und das Thema Datensicherheit wieder einmal in den Vordergrund rückt.

Auch wenn sich in den letzten Jahren – der DSGVO und verstärkter Aufklärung sei Dank –viel getan hat in Sachen Datensicherheit, sowohl in Europa als auch weltweit, ist die Dringlichkeit bei vielen Unternehmen nach wie vor nicht angekommen. Daran konnten auch Bußgelder – man denke an die 205 Millionen €-Strafe, die der Fluggesellschaft British Airways im vergangenen Sommer auferlegt wurde – nichts ändern.

Tatsache ist: Unternehmen müssen sich endlich eingestehen, dass sie unsere Daten mit herkömmlichen Sicherheitstechnologien nicht mehr ausreichend schützen können. Der Blick über den Tellerrand und das Hinterfragen bisheriger Datenschutzstrategien ist also unausweichlich.

Zahlreiche Ransomware-Attacken und insbesondere die enorme Durchschlagwirkung des E-Mail-Trojaners Emotet im vergangenen Jahr zeigen, wie schwer es Unternehmen und Behörden immer noch fällt, sowohl Sicherheitslücken in ihrer Verteidigung als auch aggressive Malware wirksam zu identifizieren und zu stoppen. Der Vorfall der 30.000 geleakten Patientendaten, die aufgrund einer Fehlkonfiguration in einem Telekom-Router im letzten Herbst für jedermann im Internet frei zugänglich waren, sind ein ideales Beispiel. Zwar drohen den betroffenen Unternehmen wegen Verstößen gegen die DSGVO eventuell saftige Bußgelder, die Opfer profitieren hierfür aber nicht.

IT-Abteilungen müssen endlich anfangen, aktiv nach potenziellen Schwachstellen und Sicherheitslücken zu suchen und gleichzeitig an jedem Endpunkt für Transparenz zu sorgen, die es erlaubt, schädliches Verhalten und Manipulationen in Echtzeit und unabhängig von Signaturen zu identifizieren und zu isolieren. Wirksamer Datenschutz ist nämlich letztlich kein Hexenwerk, sondern kann mit dem konsequenten Einsatz der richtigen Sicherheitstechnologien problemlos umgesetzt werden. Alles, was man dafür tun muss, ist traditionelle überholte IT-Sicherheit durch neue, erfolgsversprechende Techniken zu ersetzen. Ein Beispiel hierfür sind KI-basierte Endpunkt-Services, die in der Lage sind, personenbezogene Daten (PII) selbstständig zu identifizieren und einen potenziell fehlerhaften Umgang damit zu unterbinden. Fortschrittliche Lösungen bieten den IT-Abteilungen dabei sogar

kontextbezogene Einblicke in die Datenzugriffsaktivitäten, um unbefugte Zugriffe oder Datenleaks rechtzeitig zu stoppen.

Über SentinelOne

SentinelOne ist ein Pionier für autonomen Endpunktschutz und vereint die Prävention, Identifikation, Abwehr und Reaktion auf Angriffe jeglicher Art in einem einzigen Agenten. Dank dem Einsatz von künstlicher Intelligenz können Bedrohungen sowohl on-premises als auch in Cloud-Umgebungen automatisch und in Echtzeit eliminiert werden. Dabei ist die SentinelOne-Plattform ausgesprochen bedienerfreundlich und bietet eine herausragende Sichtbarkeit über alle kritischen Netzwerkvorgänge. Distributor in Deutschland, Österreich und der Schweiz ist Exclusive Networks.

Folgen Sie SentinelOne:
Website: sentinelone.com
Blog: https://www.sentinelone.com/blog/
Twitter: twitter.com/SentinelOneDE
LinkedIn: Linkedin.com/company/SentinelOne
YouTube: SentinelOne on YouTube